



DEPARTMENT OF THE NAVY
OFFICE OF THE SECRETARY
1000 NAVY PENTAGON
WASHINGTON DC 20350-1000

SECNAVINST 5239.20A
DUSN (M)/DON CIO
10 Feb 16

SECNAV INSTRUCTION 5239.20A

From: Secretary of the Navy

Subj: DEPARTMENT OF THE NAVY CYBERSPACE INFORMATION TECHNOLOGY
AND CYBERSECURITY WORKFORCE MANAGEMENT AND QUALIFICATION

Ref: See enclosure (1).

Encl: (1) References
(2) Responsibilities
(3) Glossary

1. Purpose. This instruction:

a. Establishes policy and assigns responsibilities (see enclosure (2)) for management and qualification of the Department of the Navy (DON) Cyberspace Information Technology and Cybersecurity Workforce (Cyber IT/CSWF) per reference (a).

b. Authorizes the publication of reference (b).

c. Authorizes establishment of the DON Cyber IT/CSWF Management, Oversight, and Compliance Council (Cyber IT/CSWF MOCC).

d. Establishes the Cyber IT/CSWF in alignment with guidance provided in reference (a).

2. Cancellation. SECNAVINST 5239.20.

3. Definitions. See enclosure (3).

4. Applicability

a. This instruction applies to the Offices of the Secretary of the Navy (SECNAV), the Chief of Naval Operations, and the Commandant of the Marine Corps; all U.S. Navy and U.S. Marine Corps installations, commands, activities, and field offices; and all other organizational entities within the DON.

b. This instruction specifically addresses those positions and personnel defined in enclosure (3) as:

- (1) Cyber IT WF
- (2) CSWF

c. It does not include those positions and personnel defined in enclosure (3) as:

- (1) Cyberspace Effects WF
- (2) Intelligence WF (Cyberspace)

5. Policy. It is DON policy that:

a. Commanders, Commanding Officers, Officers in Charge, and directors, hereinafter referred to as "commanders of DON organizations," shall identify all positions requiring performance of Cyber IT/CS functions.

b. All authorized users of DON Information Systems (IS) must complete approved CS awareness training annually as a condition of access prior to accessing DON information and IS. Per this instruction, commanders of DON organizations may prescribe additional command-level access requirements and may add to the standardized baseline training.

c. All Cyber IT/CSWF personnel must be qualified to perform the tasks associated with their assigned positions. This includes demonstrating foundational knowledge attained through completion of training, education, or certification programs and final qualification through demonstration of the ability to perform cybersecurity job tasks, e.g., job qualification requirement.

d. Cyber IT/CS qualification requirements will be documented in a qualification matrix, based upon a DON Cyber IT/CSWF Framework and structured by Cyber WF category, specialty, and role.

e. Foundational Cyber IT/CS knowledge will address Cyber IT/CS concepts, operating system (OS) and computing environment concepts, and technical information.

f. Foundational Cyber IT/CS knowledge may be acquired through completion of approved military training, academic degrees, commercial cybersecurity certifications, and/or other approved training and credentials.

g. Cyber IT/CS qualification requirements will be aligned with required proficiency levels.

h. A Cyber IT/CSWF Program Manager (Cyber IT/CSWF-PM) role will be established. The Cyber IT/CSWF-PM will be responsible for administration of an organization's Cyber IT/CSWF Program. Wherever possible, the Cyber IT/CSWF-PM role should be a primary duty. Only a military member or government civilian may serve as a Cyber IT/CSWF-PM. The functions of the Cyber IT/CSWF-PM may be performed for a small command by a higher level organization.

i. All Cyber IT/CS personnel will be required to maintain current qualifications through participation in annual continuous learning.

j. The identification and tracking of Cyber IT/CS positions and WF personnel qualification status will be captured and maintained in DON, Navy, and Marine Corps authoritative manpower, personnel, and readiness data bases.

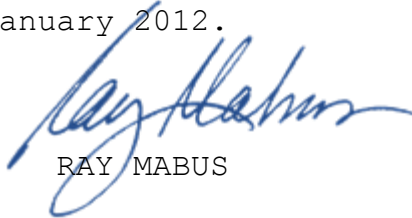
k. Each person with privileged access will be required to acknowledge special responsibilities with a Privileged Access Agreement (PAA). This agreement must be reviewed, updated, and signed annually. Personnel no longer requiring privileged access shall have their agreements removed from their records. A privileged user may be a member of either the Cyber IT or CSWF category. Designation as a privileged user is based upon the tasks and authorities assigned to the position the person holds.

l. Cyber IT/CS personnel WF qualification compliance shall be monitored by the Cyber IT/CSWF-PM. Personnel failing to maintain their qualifications shall be restricted to performing the Cyber IT/CS duties of their current positions under direct supervision of a Cyber IT/CS member with qualifications equal

to, or exceeding, the requirements of the position. Personnel failing to qualify may only be reassigned to another Cyber IT/CS position with the approval of the organization's Commander. Failure to comply will result in counseling and appropriate associated documentation. The continuing failure of a civilian employee to meet required Cyber IT/CS qualifications may be grounds for reassignment or separation under adverse action procedures.

6. Responsibilities. See enclosure (2).

7. Records Management. Records created as a result of this instruction, regardless of media and format, shall be managed per SECNAV Manual 5210.1 of January 2012.



RAY MABUS

Distribution:

Electronic only, via Department of the Navy Issuances Web site
<http://doni.documentsservices.dla.mil/>

REFERENCES

- (a) DoD Directive 8140.01 of 11 August 2015
- (b) SECNAV M-5239.2 of May 2009
- (c) 44 U.S.C. Chapter 35, Subchapter II and III Revised Federal Information Security Modernization Act (FISMA) of 2014
- (d) SECNAVINST 5239.3B
- (e) SECNAVINST 3052.2
- (f) National Security Presidential Directive (NSPD) 54/Homeland Security Presidential Directive (HSPD)-23, Cybersecurity Policy, of 8 January 2008
- (g) Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, as Amended through 15 November 2015
- (h) National Initiative for Cybersecurity Education (NICE), The National Cybersecurity Workforce Framework of 15 May 2014

RESPONSIBILITIES

1. The Department of the Navy Chief Information Officer (DON CIO) shall:

a. Carry out the Cyber IT/CSWF Management responsibilities assigned by reference (c) to the head of each Federal agency and as outlined in references (d) and (e). Accordingly, the DON CIO shall ensure DON compliance with the Cyber IT/CSWF requirements of reference (f) and related Cyber IT/CSWF policies, procedures, standards, and guidelines.

b. Set DON standards and develop Cyber IT/CSWF policies to support Cyber IT/CSWF identification, education, training, certification, and qualification. This includes oversight of the DON Cyber IT/CSWF qualification program.

c. Set DON standards and policy for DON CS awareness training.

d. Serve as the DON Cyber IT/CSWF Management and Qualification Office of Primary Responsibility (OPR), responsible for Cyber IT/CSWF guidance and oversight per reference (d).

e. Chair the Cyber IT/CSWF MOCC.

2. The DON Deputy CIO (Navy) and DON Deputy CIO (Marine Corps) shall:

a. Develop and implement Cyber IT/CSWF management and qualification programs, guidance, and procedures within their respective Service.

b. Implement DON CS awareness training. Ensure all authorized users of DON IS and networks receive initial CS awareness orientation as a condition of access, and, thereafter, complete annual refresher training to maintain CS awareness.

c. Appoint a Service Cyber IT/CSWF OPR responsible for implementation, execution, and sustainment of Service Cyber IT/CSWF management and qualification plans.

d. Implement oversight procedures to ensure Service compliance with Cyber IT/CSWF qualification requirements.

e. Employ DON, Navy, and Marine Corps manpower, personnel, and readiness databases to meet Cyber IT/CSWF management and reporting requirements.

f. Co-chair the Cyber IT/CSWF MOCC.

3. Commanders, Commanding Officers, and Officers in Charge shall:

a. Ensure the command has a Cyber IT/CSWF Management and Qualification Plan.

b. Ensure command Cyber IT/CSWF information is accurately captured in DON, Navy, and Marine Corps manpower, personnel, and readiness databases.

c. Ensure all Cyber IT/CS personnel are fully qualified per assigned Cyber IT/CS position qualification requirements.

d. Ensure all personnel with privileged access acknowledge their responsibilities with a PAA. Ensure the agreement is understood and signed by the privileged user prior to assignment and annually thereafter.

e. Ensure that personnel no longer requiring privileged access have their PAA removed from their record.

f. Ensure all contracts requiring cybersecurity contractor personnel provide detailed cybersecurity qualification requirements. Also ensure that proposed cybersecurity contractor personnel are appropriately qualified prior to the start of the contract performance period or before assignment to the contract during the course of the performance period.

g. Designate a Command Cyber IT/CSWF-PM. The Cyber IT/CSWF-PM will be responsible for the administration of the organization's Cyber IT/CSWF program. In small commands, the functions of the Cyber IT/CSWF-PM may be performed by a higher level organization.

GLOSSARY

Abbreviations and Acronyms

CS	Cybersecurity
Cyber IT/CSWF-PM	Cyber IT/Cybersecurity Workforce Program Manager
Cyber IT/CS	Cyberspace Information Technology and Cybersecurity
DoD	Department of Defense
DON	Department of the Navy
DON CIO	Department of the Navy Chief Information Officer
HSPD	Homeland Security Presidential Directive
IS	Information Systems
MOCC	Management, Oversight, and Compliance Council
NICE	National Initiative for Cyber Security Education
NSPD	National Security Presidential Directive
OPR	Office of Primary Responsibility
OS	Operating System
PAA	Privileged Access Agreement
SA	Specialty Area
SECNAV	Secretary of the Navy
U.S.	United States
WF	Workforce

Definitions

1. Authorized User. Any appropriately cleared individual with a requirement to access a Department of Defense (DoD) IS for performing or assisting in a lawful and authorized governmental function.
2. Certification. Recognition given to individuals who have met predetermined qualifications set by an agency of government, industry, or profession. Certification provides verification of an individual's knowledge and experience through evaluation and approval based on a set of standards for a specific profession or occupation's functional job levels. Each certification is designed to stand on its own and represents a certified individual's mastery of a particular set of knowledge and skills.
3. Cybersecurity. Prevention of damage to, protection of, and restoration of computers, electronic communication systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation (reference (g)).
4. Cybersecurity Category. Group of common major cybersecurity functions, comprised of one or more specialty areas (SAs), e.g., Protect and Defend, Operate and Maintain (reference (h)).
5. Cybersecurity Workforce (CSWF). Personnel who secure, defend, and preserve data, networks, net-centric capabilities, and other designated systems by ensuring appropriate security controls and measures are in place and taking internal defense actions. This includes access to system controls, monitoring, administration, and integration of cybersecurity into all aspects of engineering and acquisition of cyberspace capabilities (reference (a)).
6. Cyberspace. A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers (reference (g)).

7. Cyberspace Effects Workforce. Personnel who plan, support, and execute cyberspace capabilities where the primary purpose is to externally defend or conduct force projection in or through cyberspace (reference (a)).

8. Cyberspace Information Technology/Cybersecurity Specialty Area (Cyber IT/CS SA). A Cyberspace IT/CS SA represents an area of concentrated work, or function, within information technology and/or cybersecurity. Included in each SA are typical tasks and knowledge, skills, and abilities (reference (h)).

9. Cyber IT/CS Workforce Program Manager (Cyber IT/CSWF-PM). The Cyber IT/CSWF-PM will be responsible for the administration and management of the organization's Cyber IT/CSWF Program. The Cyber IT/CSWF-PM is responsible for the reporting, database management, and overall effectiveness of the program at commands and/or subordinate units. Wherever possible, the Cyber IT/CSWF-PM role should be a primary duty. Only military or government civilian personnel may serve as a Cyber IT/CSWF-PM. In small commands, the functions of the Cyber IT/CSWF-PM may be performed by a higher level organization.

10. Cyberspace Information Technology Workforce (Cyber IT WF). Personnel who design, build, configure, operate, and maintain information technology, networks, and capabilities. This includes actions to prioritize portfolio investments, architect, engineer, acquire, implement, evaluate, and dispose of information technology; as well as information resource management, and the management, storage, transmission, and display of data and information (reference (a)).

11. Cyberspace Workforce. Personnel who build, secure, operate, defend, and protect DoD and U.S. cyberspace resources; conduct related intelligence activities; enable future operations; and project power in or through cyberspace. It is comprised of personnel assigned to the areas of cyberspace effects, cybersecurity, cyberspace IT, and portions of the Intelligence WFs (reference (a)).

12. Privileged Access. Access to system control, monitoring, administration, criminal investigation, or compliance functions. Privileged access typically provides access to the following system controls:

- a. Access to the control functions of the IS and/or network, administration of user accounts, etc.
 - b. Access to change control parameters, e.g., routing tables, path priorities, addresses, of routers, multiplexers, and other key IS and/or network equipment or software.
 - c. Ability and authority to control and change program files, and other users' access to data.
 - d. Direct access to OS level functions that permit system controls to be bypassed or changed.
 - e. Access and authority for installing, configuring, monitoring security monitoring functions of IS and/or networks, e.g., network and/or system analyzers; intrusion detection software; firewalls, or in performance of cyber and/or network defense operations.
13. Privileged User. A user that is authorized, and therefore trusted, to perform security-relevant functions that ordinary users are not authorized to perform.
14. Proficiency. Ability to perform a specific behavior, e.g., task, learning objective, to the established performance standard in order to demonstrate mastery of the behavior. CSWF personnel follow a training progression that supports continual skill development through individual and team proficiency.